

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

JUN 21 2017

UNDER SEAL

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Information associated with Apple ID doudz@aol.com
that is stored at premises controlled by Apple Inc.

Case No. 1:17sw 350

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Apple ID doudz@aol.com that is stored at premises controlled by Apple Inc.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 793	Gathering, transmitting or losing defense information
18 U.S.C. § 794	Gathering or delivering defense information to aid a foreign government
18 U.S.C. § 1956	Laundering of monetary instruments

The application is based on these facts:

See Attached Affidavit

- ☐ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA John T. Gibbs

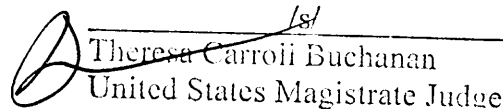


Applicant's signature

Stephen Green, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 06/21/2017


Judge's signature

Theresa Caroli Buchanan
United States Magistrate Judge

Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

City and state: Alexandria, Virginia

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID doudz@aol.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 793(e), 18 U.S.C. § 794(a), and 18 U.S.C. § 1956 and 18 U.S.C. § 1001 involving Kevin Patrick Mallory since October 13, 2011, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications between Kevin Patrick Mallory and PRC1;
- b. Any communications, files or other records containing information relating to the national defense and/or classified information;
- c. Any communications, files or other records containing U.S. Government information;
- d. Any communications, files or other records regarding tradecraft, how to obtain or deliver sensitive information, and/or how to avoid or evade detection by intelligence officials or law enforcement authorities;
- e. Any communications, files or other records regarding travel, including calendars, travel tickets, receipts, and photographs;
- f. Any communications, files or other records pertaining to any others who conspired with Kevin Patrick Mallory to release, communicate, or transmit national defense information and/or classified information;

g. Any financial records, including bank statements, account information and records of any financial transaction that may be evidence of payments for the sale of classified information;

h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

i. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

j. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

k. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

l. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and
- c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

JUN 21 2017

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
APPLE ID DOUDZ@AOL.COM)
THAT IS STORED AT PREMISES)
CONTROLLED BY APPLE, INC.)

CASE NO. 1:17 sw-350

UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Stephen Green, after being duly sworn, depose and state as follows:

1. I am a Special Agent with the FBI, and have been since 2012. Since 2012, I have been assigned to the Washington Field Office, Counterintelligence Division. Since October 2016, I investigated offenses involving espionage and the unlawful retention or disclosure of classified information. I was the affiant on the affidavit in support of a criminal complaint and arrest warrant, charging Kevin Patrick Mallory (hereinafter Mallory) with making materially false statements to Federal Bureau of Investigation (FBI) agents, in violation of 18 U.S.C. § 1001, and Gathering or Delivering Defense Information to Aid a Foreign Government, in violation of 18 U.S.C. § 794.

2. This affidavit is submitted in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop,

Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

3. Based on the facts set forth in this affidavit (and incorporating the facts contained in the Criminal Complaint Affidavit), there is probable cause that within these locations or things is evidence, more particularly described in Attachment A, of violations of federal law, including 18 U.S.C. § 793(e) (gathering, transmitting or losing defense information), 18 U.S.C. § 794(a) (gathering or delivering defense information to aid foreign government), and 18 U.S.C. § 1956 (laundering of monetary instruments) and 18 U.S.C. § 1001 (making materially false statements).

4. This affidavit is being submitted for the limited purpose of obtaining a search warrant. As a result, it does not include each and every fact observed by me or known to the government. When I assert that a statement was made by an individual, that statement is described in substance and in part, but my assertion is not intended to constitute a verbatim recitation of the entire statement. When I assert that an event occurred or a communication was made on a certain date, I mean that the event occurred or the communication was made “on or about” that date.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On April 21, 2017, on a return flight from Shanghai, China, Mallory was subject to a secondary search and interview by United States Customs and Border Protection (“CBP”) Agents at Chicago O’Hare Airport. During the interactions with CBP on April 21, 2017, Mallory’s e-mail address was identified as doudz@aol.com.

7. On or about June 19, 2017, in response to a subpoena request, Apple provided the Apple ID doudz@aol.com is associated with DS ID 12822856 and is registered to Mallory at his residence 16621 Elk Run Ct, Leesburg, Virginia. The account was created on October 13, 2011 and is currently active.

INFORMATION REGARDING APPLE ID AND iCloud¹

8. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

9. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “iCloud: iCloud storage and backup overview,” available at <https://support.apple.com/kb/PH12519>; and “iOS Security,” available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user’s Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

10. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

11. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or AOL). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

12. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

13. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

14. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is

linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

15. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud. Some of this data is stored on Apple’s servers in an encrypted form but can nonetheless be decrypted by Apple.

16. During Mallory's secondary search and interview on April 21, 2017 with CBP following a flight from Shanghai, China, Mallory was traveling with two Apple iPhones. Mallory later admitted to the FBI in an interview on May 24, 2017, that he had met with a person he believed was a People's Republic of China government agent ("PRC1") while on that April trip to China. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

17. I know that Mallory has transmitted documents classified at the TOP SECRET and at the SECRET level to PRC1. Given that Mallory previously worked at the U.S. government agency that classified these documents, and given that these documents are several years old, I believe that it is likely that Mallory maintains other documents related to his employment with the U.S. Government connected to his Apple ID. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation, to include 18 U.S.C. § 1001 and 18 U.S.C. § 794. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

18. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user

attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

19. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

20. During the May 24 meeting with the FBI agents, Mallory signed a voluntary consent form permitting the FBI to search the device provided to Mallory by PRC1, which he had brought to the meeting. At that time, the FBI extracted an image of the device, and returned the device to Mallory. The FBI conducted further technical examination of the imaged copy of the device after the interview. Identified on the device was a series of messages sent on or about May 3, 2017, where Mallory stated, “I have arranged for a USD account in another name. You can send the funds broken into 4 equal payments over 4 consecutive days...When you agree I will send you the bank I.g instructions.” Other information connected to an Apple ID may lead to

the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services, such as banking institutions, used in furtherance of the crimes under investigation or services used to communicate with PRC1. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

21. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

22. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

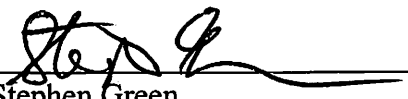
23. Based on the forgoing, I request that the Court issue the proposed search warrant.

24. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING


25. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Stephen Green
Special Agent
Federal Bureau of Investigation
Washington, DC

Subscribed and sworn to before me on June 21, 2017



/s/
Theresa Carroli Buchanan
United States Magistrate Judge

THE HONORABLE THERESA C. BUCHANAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID doudz@aol.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 793(e), 18 U.S.C. § 794(a), and 18 U.S.C. § 1956 and 18 U.S.C. § 1001 involving Kevin Patrick Mallory since October 13, 2011, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications between Kevin Patrick Mallory and PRC1;
- b. Any communications, files or other records containing information relating to the national defense and/or classified information;
- c. Any communications, files or other records containing U.S. Government information;
- d. Any communications, files or other records regarding tradecraft, how to obtain or deliver sensitive information, and/or how to avoid or evade detection by intelligence officials or law enforcement authorities;
- e. Any communications, files or other records regarding travel, including calendars, travel tickets, receipts, and photographs;
- f. Any communications, files or other records pertaining to any others who conspired with Kevin Patrick Mallory to release, communicate, or transmit national defense information and/or classified information;

g. Any financial records, including bank statements, account information and records of any financial transaction that may be evidence of payments for the sale of classified information;

h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

i. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

j. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

k. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

l. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and

c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature